IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA

v.

ALEXANDER KONSTANTINOVICH TVERDOKHLEBOV,

Defendant.

CRIMINAL NO.: 1:17-CR-9

GOVERNMENT'S MOTION TO REVOKE RELEASE ORDER AND ORDER DEFENDANT DETAINED

The defendant, Alexander Tverdokhlebov ("Tverdokhlebov" or "Defendant") was indicted by a grand jury in this district on four counts of wire fraud, arising from a scheme to steal sensitive financial information from thousands of victim computers and use that information to make fraudulent purchases and transfers of funds. On February 1, 2017, he was arrested at his residence in Los Angeles and made an initial appearance in the Central District of California. U.S. Magistrate Judge Patrick J. Walsh ordered Defendant released on bond, but stayed that order until February 7, 2017 in order to give the Government an opportunity to appeal. Judge Walsh provided that, if the Government chose to appeal, the stay would remain in effect until this Court issues its ruling on pretrial detention.

The Government believes that Defendant poses a serious risk of flight and a danger to the community. In particular, Defendant is a Russian national with no known legitimate employment and few ties to the United States. He is a member of several elite Russian-speaking cybercrime forums that provide him with a network of sophisticated co-conspirators. He has spoken to other cybercriminals in the past about his plan to store "compromising" material outside of his home to

evade law enforcement. He has strong ties to a Russian cybercriminal living in Mexico. And, during a search of his residence just last week, law enforcement found keys to safety deposit boxes at three different banks, which Defendant's partner said he opened in case of a "bad day." A search of those boxes yielded approximately **$172,000 in $100 bills**.

For all these reasons, the United States believes there is a significant danger that Defendant could flee to Mexico, and ultimately to Russia or Eastern Europe, from which extradition is unlikely. Accordingly, the Government respectfully requests, pursuant to 18 U.S.C. § 3145(a), that the Court revoke the release order and direct that Defendant be detained pending trial.

BACKGROUND

Defendant has been in the business of international cybercrime from at least 2008 until the present. He has been a member of several elite Russian-speaking cybercrime forums whose purpose is to facilitate crime by, for instance, allowing members to buy and sell stolen personal information, hacking tools, and money laundering services. These forums restrict membership to individuals who can prove their criminal bonafides by, inter alia, having current members vouch for their criminal history. During his years of activity on these forums, Defendant has advertised several illegal schemes, including schemes to launder money and to sell stolen credit card information. The scheme charged in the indictment involved the operation of a "botnet," which is a group of infected computers from which sensitive information can be stolen. Defendant used his botnet—which he once bragged included 10,000 infected computers—to steal passwords to online bank accounts and make fraudulent transfers and purchases.

ARGUMENT

I. Legal Standard

Section 3142 of Title 18 of the United States Code, enacted as part of the Bail Reform Act of 1984, 18 U.S.C. §§ 3141–3156 (the "Bail Reform Act"), requires that an accused be detained pending trial where, following a hearing in accordance with section 3142(f), "the judicial officer finds that no condition or combination of conditions will reasonably assure the appearance of the person as required and the safety of any other person and the community." 18 U.S.C.S. § 3142(e)(1). The factors that a judicial officer must consider "in determining whether there are conditions of release that will reasonably assure the appearance of the person as required" include: "the nature and circumstances of the offense charged"; "the weight of the evidence against the person"; "the history and characteristics of the person," including his family ties, financial resources, and community ties." 18 U.S.C.S. § 3142(g). With regard to the risk of flight as a basis for detention, the government "must prove by a preponderance of the evidence that no combination of conditions will reasonably assure the defendant's appearance at future court proceedings." *United States v. Maniscan*, 2015 WL 7455541, at *1 (E.D. Va. Nov. 23, 2015).

A district court reviews the ruling of a magistrate judge on pretrial detention *de novo*. *See United States v. Williams,* 753 F.2d 329, 331 (4th Cir. 1985).

II. Totality of the Circumstances Demonstrates Defendant is a Serious Flight Risk

Defendant is a Russian-born hacker with criminal affiliates in foreign jurisdictions, a sophisticated criminal who is skilled at obtaining funds through fraud, and an individual facing a significant sentence of imprisonment. These three facts weigh heavily toward pretrial detention. *See United States v. Stanford*, 394 F. App'x 72, 75 (5th Cir. 2010) (holding that the factors

"compellingly call for . . . pretrial detention," where the defendant had "the means, the motive, and the money to flee," including "an international network of contacts," a "primary residence in Antigua and Barbuda for the past fifteen years, and . . . little family ties in Houston"); *United States v. Mehmood*, 358 Fed. Appx. 767 (8th Cir. 2010) (pretrial detention appropriate due to flight risk in visa fraud case where defendant was Pakistani, had used aliases, and had property and financial interests in Canada). Moreover, Defendant's efforts to deceive law enforcement make it unlikely he will follow through on any promise to appear at a future court date in this District.

A. Nature and Circumstances of the Charged Offenses

Defendant is an extremely sophisticated and well-connected cybercriminal. Since at least 2008, Defendant has been a member of several of the most exclusive Russian-speaking cybercrime forums. These forums restrict membership to prolific cybercriminals and are designed to provide their members with access to co-conspirators with the ability and willingness to hack computer systems, produce fraudulent documents, buy and sell stolen social security numbers and credit/debit card numbers, and launder money. Unlike other cybercriminals whose participation on these forums may have been limited in duration, Defendant has been active on such forums from 2008 until just weeks ago.

Defendant's active participation on the forums means he has access to experts in counterfeiting, identity theft, and money laundering. Indeed, a review of Defendant's affiliations revealed contacts with some of the world's most notorious cybercriminals. For instance, the charges in the indictment stem from a scheme between Defendant and Vadim Polyakov, who was extradited to the United States from Spain in 2015 and has since pled guilty in New York to hacking-related crimes. Defendant's "voucher" for entry onto one elite cybercrime forum was a Ukrainian cybercriminal, who has since been arrested in Israel and is currently facing extradition

to the United States. And, most relevant here, the Government is aware of a Russian-born cybercriminal who previously lived near Defendant in Southern California but now resides in Mexico. Defendant was close enough to this individual to "vouch" for his admission to an elite cybercrime forum in 2012, telling the membership that he has known him for five years, that he is a profession "carder" (meaning, someone who sells stolen credit card numbers), and would "be an asset to the forum." In addition, the Government has Western Union records from 2008 showing Defendant's transfer of funds to this individual. Defendant's worldwide criminal connections could serve him well should he decide to flee.

B. The Weight of the Evidence

The evidence against Defendant is overwhelming. The Government is in possession of messages between Defendant and Polyakov regarding their "botnet" scheme. The Government was able to identify Defendant as the person in these chats with Polyakov because Defendant gave his first name, his home address, his girlfriend's full name, and e-mail addresses and phone numbers linked to him. In a *Mirandized* post-arrest interview, Defendant acknowledged ownership of an e-mail account that was used to instruct lower-level criminals on how to receive and transfer stolen funds. Finally, Defendant's possession of $172,000 in unexplained cash, as well his receipt of large wire transfers, described more fully below, is strong evidence that he is indeed the cybercriminal that he is accused of being.

C. History and Characteristics of Defendant

Defendant's strong ties to foreign countries, access to funds, and efforts to deceive law enforcement indicate that he is a serious flight risk.

1. Ties to Russia, Mexico, and China

Defendant has strong ties to Russia. He was born in Russia, has citizenship in Russia, and has family currently living in Russia. Defendant has strong ties to Russian cybercriminal affiliates currently based in Russia. Defendant has also worked closely with a Russian cybercriminal currently living in Mexico who is believed will come to Defendant's aid if Defendant tries to flee the country. Last, bank records show that Defendant received **approximately $1 million** in wire transfers from Russia and China.

The fact that Defendant is currently a U.S. citizen does not undercut the Government's belief that Defendant poses a serious flight risk. Defendant obtained his U.S. citizenship shortly after marriage to a U.S. citizen in 2009. However, investigation has revealed that he has since divorced his American wife, and that she received a large transfer of money shortly after their marriage in 2009. Defendant's only significant tie to the United States is a Russian-born woman with whom he appears to have been in a relationship with for much of the time prior to his marriage in 2009 and after.

2. Access to Funds

Defendant has significant financial resources, is capable of obtaining more funds through fraudulent means, and has carefully planned how to evade law enforcement. Several years ago, he discussed with a co-conspirator the use a "deposit box" to store "compromising things" outside of the home. The following is a reproduction of the chat messages between the two individuals:[1]

[1] The chat messages are reproduced in both the original Russian and the English translation. Both Defendant and his co-conspirator sent the messages under online aliases. In order to avoid compromising the defendant's online identity, the Government has replaced their aliases with "Defendant" and "Co-conspirator."

[Defendant] (01:12:11 19/04/2009)
да хз... все равно палево какой то материал дома хранить... начнуть копать и все... я вообще параноик....%)

darn who knows... it is necessary to keep some sort of compromising material at home... (they) start digging deeper and that is it... I am a real paranoid....%)

---------->-
[Co-conspirator] (01:13:29 19/04/2009)
:-) селф сторадж тебе поможет или банковская ячейка, правда ячейку полицаи выпалят

:-) self storage could help you or a bank deposit box, although it is true that the police can find a bank deposit box

----------<-
[Defendant] (01:14:02 19/04/2009)
они имеют право банк ячейку выставить?

they have the right to access a deposit box?

----------<-
[Defendant] (01:14:07 19/04/2009)
:-(

:-(

----------<-
[Defendant] (01:14:23 19/04/2009)
у меня есть... я там паливо храню=))

i have one.... i keep compromising things there=))

---------->-
[Co-conspirator] (01:15:35 19/04/2009)
:-))) мощно , насколько я знаю да, могут и ячейку вынести, и деньги списать...но возможно это при наличии решения судьи "с конфискацией", не уверен

:-))) solid , as far as i know, they can recover a deposit box, and take the money...but perhaps it is only with a court decision "with forfeiture", i'm not sure

---------->-
[Co-conspirator] (01:16:06 19/04/2009)
бля сними селф сторадж, их же миллион везде и храни там палево, это частная контора, твое имя ни в каких базах лежать не будет

darn rent a self storage, there are millions of them all over the place and store compromising material there, it is a private operation, your name will not be an any databases

----------<-
[Defendant] (01:16:21 19/04/2009)
да пох... думаю не дойдет=))) не миллионы же пиздим... пока...

screw that... i don't think it will get to that=))) we are not stealing millions... yet...

---------->-
[Co-conspirator] (01:16:42 19/04/2009)
а по банкам запросить что есть на имя человека полиция в пять сек сделает...

whereas it takes the police five seconds to ask banks what they have in the name of an individual...

----------<-
[Defendant] (01:17:19 19/04/2009)
ну мое имя вроде нигде не светится, а если что случится, я думаю и селф сторадж не поможет=))

well my name does not appear anywhere, and if something happens, i don't think that self storage will help=))

Law enforcement recovered five keys corresponding to safe-deposit boxes during their search of Defendant's residence. When law enforcement questioned Defendant's Russian-born partner about the safe-deposit boxes, she stated that Defendant told her he was opening one of them in her name in preparation for a "bad day."

A search of three of the safe-deposit boxes whose keys were discovered in Defendant's residence revealed a total of $172,000 in $100 bills spread across the three boxes. One of the three boxes contained a key believed to correspond to a fourth safe-deposit box located in Las Vegas. Given that bank records have demonstrated that approximately $1 million flowed through one of Defendant's bank accounts, the Government believes there is a substantial likelihood that Defendant is holding assets in offshore bank accounts and other accounts not yet discovered.

3. Dishonesty to the Court and Law Enforcement

After Defendant's arrest, Defendant gave a voluntary, *Mirandized* interview in which he made several statements that were misleading at best. He disavowed technological sophistication, stating that he did not know whether his devices were encrypted and, if they were, the password was "qwerty" (an unsophisticated password comprised of the first five letters on the top left side of a key board). A search of Defendant's home, however, returned laptops, cellular phones, hard drives, and other digital media device, almost all of which were heavily encrypted, suggesting a level of technological sophistication proportional to the sophistication of his scheme. Defendant did acknowledge ownership of an e-mail account which was used for a money laundering scheme. But Defendant claimed that this e-mail account was created by someone else who gave it to Defendant because, at the time, Defendant did not know how to create his own e-mail account. This, too, was untruthful, as the Government has evidence of Defendant using this account during the commission of the charges offenses. Finally, Defendant stated that his businesses make little money and that he is a "consultant," but neglected to mention his deposit boxes with $172,000 cash or his large wire transfers. Defendant's attempts at deception indicate that he cannot be relied upon to travel to this District of his own accord to face the pending charges.

CONCLUSION

For the forgoing reasons, the United States respectfully requests, pursuant to 18 U.S.C. § 3145(a)(1), that the Court revoke the Magistrate Judge's order and direct that Defendant be detained pending trial in this Court.

Respectfully submitted,

Dana J. Boente
United States Attorney

By: _____
Laura Fong
Kellen S. Dwyer
Assistant United States Attorneys

February 6, 2017

Certificate of Service

I hereby certify that on February 6, 2017, served the forgoing document on the following defense counsel of record[2] via e-mail:

Lisa Shinar LaBarre
Deputy Federal Public Defender
321 E. 2nd Street
Los Angeles, CA 90012
Phone: (213) 894-1476
Fax: (213) 894-7566
E-mail: Lisa_Labarre@fd.org

By: _____
Laura Fong
Kellen S. Dwyer
Assistant United States Attorneys
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, Virginia 22314
(703) 299-3934 office, (703) 299-3981 fax
laura.fong@usdoj.gov
kellen.dwyer@usdoj.gov

[2] The Government has contacted the Federal Public Defender's Office in the Eastern District of Virginia and has been informed that the Federal Public Defender's Office in this District will be working to obtain local counsel for Defendant.